12 LOẠI MÃ ĐỘC

I.Mã độc là gì? Tổng quan về mã độc

Mã độc hay “Malicious software” là một loại phần mềm được tạo ra và chèn vào hệ thống một cách bí mật với mục đích thâm nhập, phá hoại hệ thống hoặc lấy cắp thông tin, làm gián đoạn, tổn hại tới tính bí mật, tính toàn vẹn và tính sẵn sàng của máy tính nạn nhân. Mã độc được phân thành nhiều loại tùy theo chức năng, cách thức lây nhiễm, phá hoại: virus, worm, trojan, rootkit …

Mọi người hay bị nhầm lẫn với 1 khái niệm khác là Virus máy tính. Thực tế, virus máy tính chỉ là 1 phần nhỏ trong khái niệm mã độc. Virus máy tính hiểu đơn thuần cũng là một dạng mã độc nhưng sự khác biệt ở chỗ virus máy tính có KHẢ NĂNG TỰ LÂY LAN.

Các loại mã độc càng ngày càng phức tạp từ cách thức lây nhiễm, phương pháp ẩn mình, cách thức thực hiện các hành vi nguy hiểm… Giới hạn giữa các loại mã độc ngày càng hạn hẹp vì bản thân các mã độc cũng phải có sự kết hợp lẫn nhau để hiệu quả tấn công là cao nhất.

Sau đây, tôi xin trình bày một số khái niệm về mã độc dựa trên 3 yếu tố chính: Chức năng, Đối tượng lây nhiễm, Đặc trưng của mã độc.

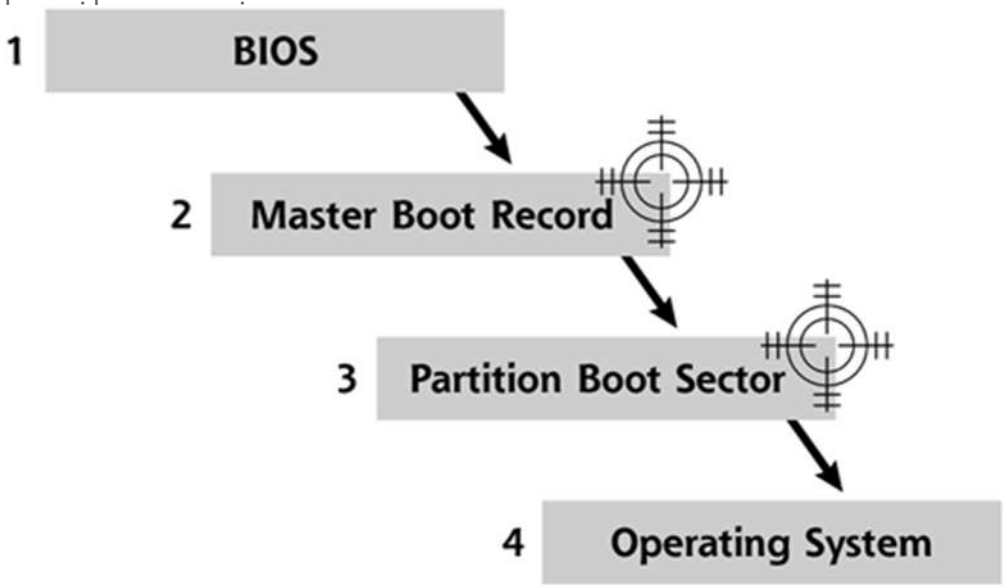
II.12 Loại mã độc phổ biến

1.Boot virus

Boot virus hay còn gọi là virus boot, là loại virus lây vào boot sector hoặc master boot record của ổ đĩa cứng. Đây là các khu vực đặc biệt chứa các dữ liệu để khởi động hệ thống, nạp các phân vùng.

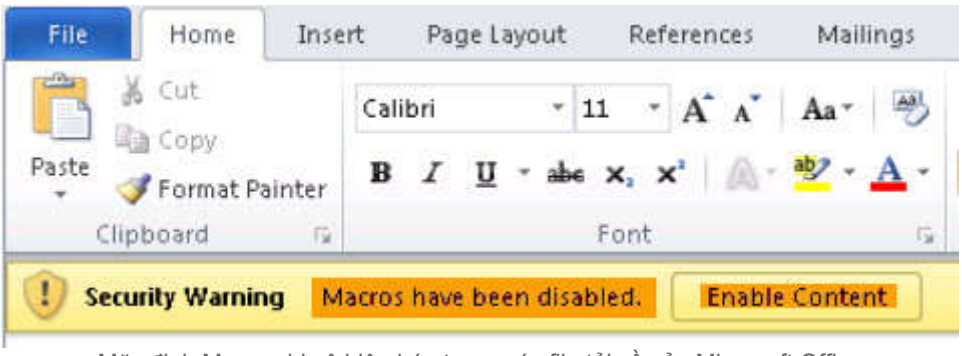
Boot Virus được thực thi trước khi hệ điều hành được nạp lên vì vậy nó hoàn toàn độc lập với hệ điều hành. B-Virus có nhược điểm là khó viết do không thể sử dụng các dịch vụ, chức năng có sẵn của hệ điều hành và kích thước virus bị hạn chế bởi kích thước của các sector (mỗi sector chỉ có 512 byte).

Ngày nay gần như không còn thấy sự xuất hiện của Boot Virus do đặc điểm lây lan chậm và không phù hợp với thời đại Internet.



2.Macro virus

Đây là loại virus đặc biệt tấn công vào chương trình trong bộ Microsoft Office của Microsoft: Word, Excel, Powerpoint. Macro là tính năng hỗ trợ trong bộ công cụ văn phòng Microsoft Office cho phép người sử dụng lưu lại các công việc cần thực hiện lại nhiều lần. Thực tế hiện nay cho thấy virus macro gần như đã “tuyệt chủng”.



Mặc định Macros bị vô hiệu hóa trong các file tải về của Microsoft Office

3.Scripting virus

Scripting virus là loại virus được viết bằng các ngôn ngữ script (kịch bản) như VBScript, JavaScript, Batch script. Những loại virus này thường có đặc điểm dễ viết, dễ cài đặt. Chúng thường tự lây lan sang các file script khác, thay đổi nội dung cả các file html để thêm các thông tin quảng cáo, chèn banner … Đây cũng là một loại virus phát triển nhanh chóng nhờ sự phổ biến của Internet.

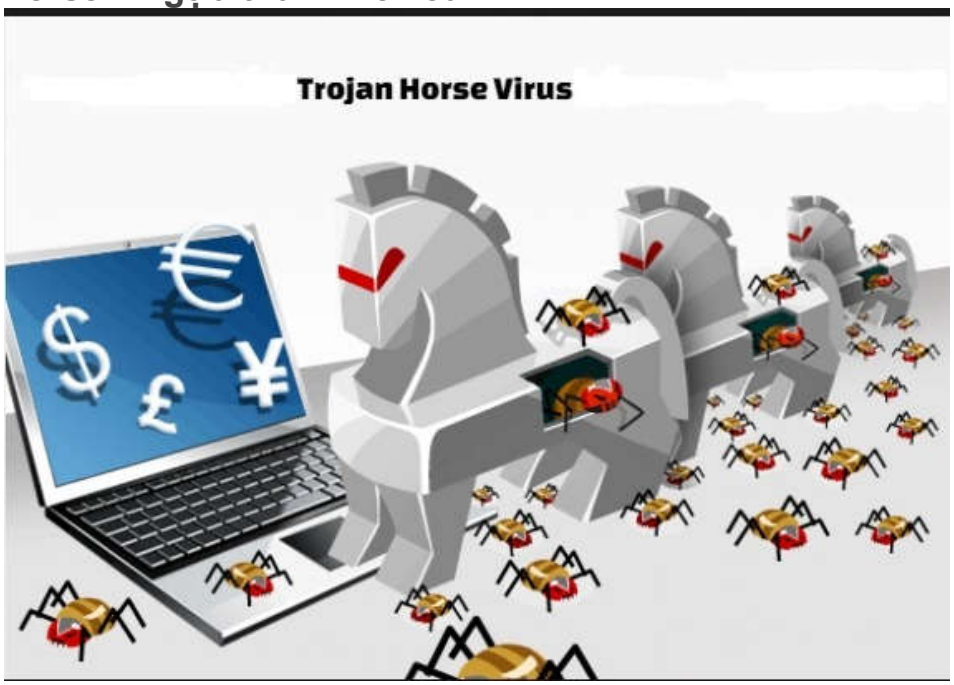
4.File Virus

Virus này chuyên lây vào các file thực thi (ví dụ file có phần mở rộng .com, .exe, .dll) một đoạn mã để khi file được thực thi, đoạn mã virus sẽ được kích hoạt trước và tiếp tục thực hiện các hành vi phá hoại, lây nhiễm.

Loại virus này có đặc điểm lây lan nhanh và khó diệt hơn các loại virus khác do phải xử lý cắt bỏ, chỉnh sửa file bị nhiễm.

File Virus có nhược điểm là chỉ lây vào một số định dạng file nhất định và phụ thuộc vào hệ điều hành. F-Virus vẫn tồn tại tới ngày nay với những biến thể ngày càng trở nên nguy hiểm, phức tạp hơn.

5.Trojan horse – ngựa thành Tơ roa



trojan horse virus

Tên của loại virus này được lấy theo một điển tích cổ. Trong cuộc chiến với người Tơ-roa, các chiến binh Hy Lạp sau nhiều ngày không thể chiếm được thành đã nghĩ ra một kế, giảng hòa rồi tặng người dân thành Tơ-roa một con ngựa gỗ khổng lồ. Sau khi ngựa gỗ được đưa vào thành, đêm đến các chiến binh Hy Lạp từ trong ngựa gỗ chui ra đánh chiếm thành.
Đây cũng chính là cách mà các Trojan horse (gọi tắt là Trojan) áp dụng: các đoạn mã của Trojan được "che giấu" trong các loại virus khác hoặc trong các phần mềm máy tính thông thường để bí mật xâm nhập vào máy nạn nhân. Khi tới thời điểm thuận lợi chúng sẽ tiến hành các hoạt động ăn cắp thông tin cá nhân, mật khẩu, điều khiển máy tính nạn nhân … Bản chất của Trojan là không tự lây lan mà phải sử dụng phần mềm khác để phát tán.
Dựa vào cách hoạt động ta có thể phân chia Trojan thành các loại sau: BackDoor, Adware và Spyware.

6.BackDoor

Phần mềm BackDoor (cửa sau) là một dạng Trojan khi thâm nhập vào máy tính nạn nhân sẽ mở ra một cổng dịch vụ cho phép kẻ tấn công điều khiển các hoạt động ở máy nạn nhân. Kẻ tấn công có thể cài các phần mềm BackDoor lên nhiều máy tính khác nhau thành một mạng lưới các máy bị điều khiển – Bot Net – rồi thực hiện các vụ tấn công từ chối dịch vụ (DoS – Denial of Service).

7.Adware và Spyware

Đây là loại Trojan khi xâm nhập vào máy tính với mục đích quảng cáo hoặc "gián điệp". Chúng đưa ra các quảng cáo, mở ra các trang web, thay đổi trang mặc định của trình duyệt (home page) … gây khó chịu cho người sử dụng. Các phần mềm này cài đặt các phần mềm ghi lại thao tác bàn phím (key logger), ăn cắp mật khẩu và thông tin cá nhân …

8.Worm – sâu máy tính

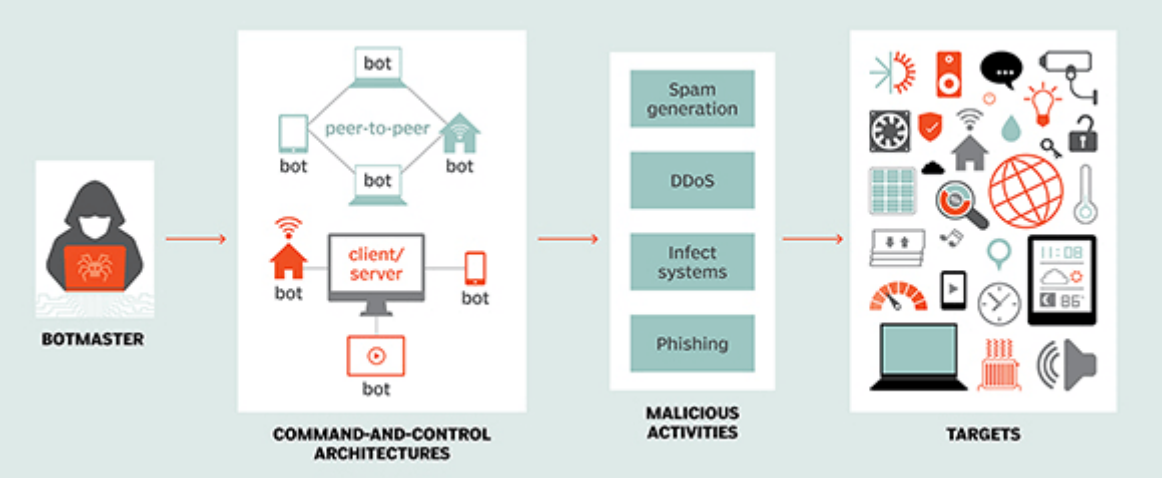
Cùng với các loại **mã độc máy tính** như Trojan, WannaCry, Worm (sâu máy tính) là loại virus phát triển và lây lan mạnh mẽ nhất hiện nay nhờ mạng Internet. Vào thời điểm ban đầu, Worm được tạo ra chỉ với mục đích phát tán qua thư điện tử – email. Khi lây vào máy tính, chúng thực hiện tìm kiếm các sổ địa chỉ, danh sách email trên máy nạn nhân rồi giả mạo các email để gửi bản thân chúng tới các địa chỉ thu thập được. Các email do worm tạo ra thường có nội dung "giật gân", hoặc "hấp dẫn", hoặc trích dẫn một email nào đó ở máy nạn nhân để ngụy trang. Điều này khiến các email giả mạo trở nên "thật" hơn và người nhận dễ bị đánh lừa hơn. Nhờ những email giả mạo đó mà Worm lây lan mạnh mẽ trên mạng Internet theo cấp số nhân.
Bên cạnh Worm lây lan theo cách truyền thống sử dụng email, Worm hiện nay còn sử dụng phương pháp lân lan qua ổ USB. Thiết bị nhớ USB đã trở nên phổ biến trên toàn thế giới do lợi thế kích thước nhỏ, cơ động và trở thành phương tiện lây lan lý tưởng cho Worm.
Dựa đặc điểm lây lan mạnh mẽ của Worm, những kẻ viết virus đã đưa thêm vào Worm các tính năng phá hoại, ăn cắp thông tin…, Worm đã trở thành "bạn đồng hành" của những phần mềm độc hại khác như BackDoor, Adware…

9.Rootkit

Rootkit ra đời sau các loại virus khác, nhưng rootkit lại được coi là một trong những loại virus nguy hiểm nhất.
Bản thân rootkit không thực sự là virus, đây là phần mềm hoặc một nhóm các phần mềm máy tính được giải pháp để can thiệp sâu vào hệ thống máy tính (nhân của hệ điều hành hoặc thậm chí là phần cứng của máy tính) với mục tiêu che giấu bản thân nó và các loại phần mềm độc hại khác.
Với sự xuất hiện của rootkit, các phần mềm độc hại như trở nên "vô hình" trước những công cụ thông thường thậm chí vô hình cả với các phần mềm diệt virus. Việc phát hiện mã độc và tiêu diệt virus trở nên khó khăn hơn rất nhiều trước sự bảo vệ của rootkit – vốn được trang bị nhiều kĩ thuật mới hiện đại.
Xuất hiện lần đầu trên hệ thống Unix từ khá lâu, nhưng kể từ lần xuất hiện "chính thức" trên hệ điều hành Windows vào năm 2005, Rootkit đang dần trở nên phổ biến và trở thành công cụ che giấu hữu hiệu cho các loại phần mềm độc hại khác.

10.Botnet

Là những máy tính bị nhiễm virus và điều khiển bởi Hacker thông qua Trojan, virus… Hacker lợi dụng sức mạnh của những máy tính bị nhiễm virus để thực hiện các hành vi tấn công, phá hoại, ăn cắp thông tin. Thiệt hại do Botnet gây ra thường rất lớn.



Kiến trúc mạng botnet

11.Biến thể

Một hình thức trong cơ chế hoạt động của virus là tạo ra các biến thể của chúng. Biến thể của virus là sự thay đổi mã nguồn nhằm các mục đích tránh sự phát hiện của phần mềm diệt virus hoặc làm thay đổi hành động của nó.

12.Virus Hoax

Đây là các cảnh báo giả về virus. Các cảnh bảo giả này thường núp dưới dạng một yêu cầu khẩn cấp để bảo vệ hệ thống. Mục tiêu của cảnh báo virus giả là cố gắng lôi kéo mọi người gửi cảnh báo càng nhiều càng tốt qua email. Bản thân cảnh báo giả là không gây nguy hiểm trực tiếp nhưng những thư gửi để cảnh báo có thể chữa mã độc hại hoặc trong cảnh báo giả có chứa các chỉ dẫn về thiết lập lại hệ điều hành, xoá file làm nguy hại tới hệ thống. Kiểu cảnh báo giả này cũng gây tốn thời gian và quấy rối bộ phận hỗ trợ kỹ thuật khi có quá nhiều người gọi đến và yêu cầu dịch vụ.

Ngày nay, sự phát triển mạnh mẽ của Internet đang tạo ra một môi trường hoạt động và lây lan lý tưởng cho các loại phần mềm độc hại. Bên cạnh đó, các hướng dẫn chi tiết, các loại công cụ để tạo virus ngày càng nhiều, xuất hiện tràn lan trên mạng toàn cầu. Đây là những yếu tố thuận lợi cho sự phát triển và lây lan mạnh mẽ của virus, mã độc. Chính vì vậy những phân loại trên đây chỉ mang tính tương đối, các loại virus đang theo xu hướng “kết hợp” lại với nhau, tạo thành những thế hệ virus mới với nhiều đặc tính hơn, khả năng phá hoại cao hơn, nguy hiểm hơn và khó bị phát hiện hơn. Vì vậy các phần mềm diệt virus có vai trò rất quan trọng, đảm bảo môi trường làm việc an toàn cho người sử dụng máy tính.

Nguồn tham khảo: https://securitybox.vn/2161/12-loai-ma-doc-pho-bien/